

AMENDMENT TO THE CLAIMS

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

LISTING OF CLAIMS:

Claims 1-4 (canceled).

Claim 5 (Currently Amended) A method for protecting a network server from being used as the basis of an attack on a network client, the method comprising:

scanning a trusted portion of said network server to find executable commands inserted by an unwanted party, said executable commands being associated with a selected programming language, wherein said trusted portion is a subset of said network server; and,

at least one of editing and removing at least a portion of said executable commands,

wherein said at least one of editing and removing comprises at least one of

rendering said executable commands unexecutable by said network client by removing a character of said executable commands; and

rendering said executable commands unexecutable by said network client by replacing particular characters within said executable commands

~~such that said executable commands still remain in said trusted portion, but cannot be executed by said network client, wherein if editing, said editing of said executable commands comprises replacing particular characters within said executable commands.~~

Claim 6 (canceled)

Claim 7 (canceled)

Claim 8 (Previously Presented) The method of Claim 5, further comprising rejecting a request when said request contains said executable commands having a hostile character.

Claim 9 (Previously Presented) The method of Claim 5, further comprising logging said executable commands to form a security log.

Claim 10 (Previously Presented) The method of Claim 9, further comprising reviewing said security log to determine whether said executable commands are hostile.

Claim 11 (Previously Presented) The method of Claim 5, wherein said scanning is accomplished during an electronic purchase transaction.

Claim 12 (Previously Presented) The method of Claim 11, wherein said electronic purchase transaction is conducted using a digital wallet.

Claims 13-50 (canceled).

Claim 51 (Previously Presented) The method of Claim 5, wherein said executable commands cause an unwanted action when executed.

Claim 52 (Previously Presented) The method of Claim 5, wherein said executable commands are malicious.

Claim 53 (Previously Presented) The method of Claim 5, further comprising receiving a request for a connection at said network server from said network client.

Claim 54 (Previously Presented) The method of Claim 53, further comprising verifying that a response from said network server to said network client is void of said executable commands.

Claim 55 (Previously Presented) The method of Claim 54, further comprising providing said response from said network server to said network client.

Claim 56 (Previously Presented) The method of Claim 5 wherein said programming language comprises javascript.

Claim 57 (Currently Amended) A method for prevention of a network attack comprising:
sending, from a network client, a request for a connection to a network server, wherein said network server scans a trusted portion of said network server to find an executable command inserted by an unwanted party into said request, said executable command being associated with a selected programming language, wherein said trusted portion is a subset of

said network server; and, said network server performs at least one of the steps of editing and removing at least a portion of said executable command for insertion into a response, wherein said at least one of editing and removing comprises at least one of: rendering said executable commands unexecutable by said network client by removing a character of said executable commands; and rendering said executable commands unexecutable by said network client by replacing particular characters within said executable commands,

~~such that said executable command still remains in said trusted portion, but cannot be executed by said network client; and wherein if editing, said editing of said executable commands comprises replacing particular characters within said executable commands; and, receiving, by said network client, said response from said network server.~~

Claim 58 (Currently Amended) The method claim 1, wherein said rendering said executable commands unexecutable by said network client by replacing particular characters within said executable commands editing comprises converting a script format character to another character, wherein said script format character identifies a block of code ~~encodes a signal to execute code.~~

Claim 59 (Currently Amended) The method claim 1, wherein said rendering said executable commands unexecutable by said network client by removing a character of said executable commands ~~removing~~ comprises removing a script format character, wherein said script format character identifies a block of code ~~encodes a signal to execute code.~~